

Re: Confounded by PAM and OpenSSH on Solaris 10

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2006-05/msg00002.html>

- *From:* "elroy.deng@xxxxxxxxxx" <elroy.deng@xxxxxxxxxx>
 - *Date:* 1 May 2006 19:52:05 -0700
-

Hi,

If anyone can help me understand OpenSSH and PAM and the various

Which version of OpenSSH? The PAM behaviour has changed (improved, I hope :-)) over time. An overview is in the faq (<http://www.openssh.com/faq.html#3.15>) but the details vary with the version.

I apologize. I wanted to provide you with all of the information as well as write a post that made sense so I edited out the version information. I am running "OpenSSH_4.3p2, OpenSSL 0.9.8a 11 Oct 2005".

user2 is unable to login and instead of calling pam_sm_chauthtok() OpenSSH calls passwd().

That happens when you use password authentication and privilege separation together. When you use password authentication, sshd doesn't have the ability to interact with the user until very late in the login process (ie after the pty is allocated) and when privsep is in use, has long since given up the privilege it would need to call pam_chauthtok (and have it work, anyway).

Either use ChallengeResponseAuthentication (preferred) or disable UsePrivilegeSeparation.

I apologize again. I assumed priv sep was disabled by default. I shut it off and set "ChallengeResponseAuthentication no" and "PasswordAuthentication yes" and everything seems to work as intended.

Re: Confounded by PAM and OpenSSH on Solaris 10

user1 gets the 'account has expired' message but it does not close the connection until three attempts are made!

I think that this no longer happens in 4.3p2.

Well I am going to paste some more stuff. Since you say that ChallengeResponseAuthentication is preferred here are the issues i am having with it enabled. Here is my configuration:

```
### START /usr/local/etc/sshd_config ###
[Mon May 01|14:04:59][root@unknown:/]
$ cat /usr/local/etc/sshd_config | grep -v '^#'
Port 2022
Protocol 2
PasswordAuthentication no
ChallengeResponseAuthentication yes
UsePAM yes
UsePrivilegeSeparation no
Subsystem sftp /usr/local/libexec/sftp-server
[Mon May 01|14:05:38][root@unknown:/]
### END /usr/local/etc/sshd_config ###
```

user1 reports expired and returns PAM_ACCT_EXPIRED. I am not kicked out.

Here are the dumps!

```
### START server command ###
$ /usr/local/sbin/sshd -ddd -D > /tmp/sshdebug.txt 2>&1
[Mon May 01|14:15:38][root@unknown:/]
$
### END server command ###
```

```
### START client view ###
[Mon May 01|14:05:38][root@unknown:/]
$ ssh -p 2022 -l user1 localhost
Password:
User account has expired!
```

```
Password:
User account has expired!
```

```
Password:
User account has expired!
```

```
Permission denied (publickey,keyboard-interactive).
[Mon May 01|14:15:38][root@unknown:/]
```

Re: Confounded by PAM and OpenSSH on Solaris 10

END client view

START sshd debug

```
$ cat /tmp/sshdebug.txt
debug2: load_server_config: filename /usr/local/etc/sshd_config
debug2: load_server_config: done config len = 265
debug2: parse_server_config: config /usr/local/etc/sshd_config len 265
debug1: sshd version OpenSSH_4.3p2
debug3: Not a RSA1 key file /usr/local/etc/ssh_host_rsa_key.
debug1: read PEM private key done: type RSA
debug1: private host key: #0 type 1 RSA
debug3: Not a RSA1 key file /usr/local/etc/ssh_host_dsa_key.
debug1: read PEM private key done: type DSA
debug1: private host key: #1 type 2 DSA
debug1: rexec_argv[0]='/usr/local/sbin/sshd'
debug1: rexec_argv[1]='-ddd'
debug1: rexec_argv[2]='-D'
debug2: fd 3 setting O_NONBLOCK
debug1: Bind to port 2022 on ::.
Server listening on :: port 2022.
debug2: fd 4 setting O_NONBLOCK
debug1: Bind to port 2022 on 0.0.0.0.
Server listening on 0.0.0.0 port 2022.
debug1: fd 5 clearing O_NONBLOCK
debug1: Server will not fork when running in debugging mode.
debug3: send_rexec_state: entering fd = 10 config len 265
debug3: ssh_msg_send: type 0
debug3: send_rexec_state: done
debug1: rexec start in 5 out 5 newsock 5 pipe -1 sock 10
debug1: inetd sockets after dupping: 3, 3
Connection from 127.0.0.1 port 32861
debug1: Client protocol version 2.0; client software version
Sun_SSH_1.1
debug1: no match: Sun_SSH_1.1
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_4.3
debug2: fd 3 setting O_NONBLOCK
debug1: list_hostkey_types: ssh-rsa,ssh-dss
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug2: kex_parse_kexinit:
diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
debug2: kex_parse_kexinit: ssh-rsa,ssh-dss
debug2: kex_parse_kexinit:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc
debug2: kex_parse_kexinit:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc
debug2: kex_parse_kexinit:
hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@xxxxxxxxxxx,hmac-sha1-96,hmac-md5-96
debug2: kex_parse_kexinit:
hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@xxxxxxxxxxx,hmac-sha1-96,hmac-md5-96
```

Re: Confounded by PAM and OpenSSH on Solaris 10

```
debug2: kex_parse_kexinit: none,zlib@xxxxxxxxxxxx
debug2: kex_parse_kexinit: none,zlib@xxxxxxxxxxxx
debug2: kex_parse_kexinit:
debug2: kex_parse_kexinit:
debug2: kex_parse_kexinit: first_kex_follows 0
debug2: kex_parse_kexinit: reserved 0
debug2: kex_parse_kexinit:
diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
debug2: kex_parse_kexinit: ssh-rsa,ssh-dss
debug2: kex_parse_kexinit:
aes128-ctr,aes128-cbc,arcfour,3des-cbc,blowfish-cbc
debug2: kex_parse_kexinit:
aes128-ctr,aes128-cbc,arcfour,3des-cbc,blowfish-cbc
debug2: kex_parse_kexinit: hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96
debug2: kex_parse_kexinit: hmac-md5,hmac-sha1,hmac-sha1-96,hmac-md5-96
debug2: kex_parse_kexinit: none,zlib
debug2: kex_parse_kexinit: none,zlib
debug2: kex_parse_kexinit: i-default
debug2: kex_parse_kexinit: i-default
debug2: kex_parse_kexinit: first_kex_follows 0
debug2: kex_parse_kexinit: reserved 0
debug2: mac_init: found hmac-md5
debug1: kex: client->server aes128-ctr hmac-md5 none
debug2: mac_init: found hmac-md5
debug1: kex: server->client aes128-ctr hmac-md5 none
debug1: SSH2_MSG_KEX_DH_GEX_REQUEST received
debug1: SSH2_MSG_KEX_DH_GEX_GROUP sent
debug2: dh_gen_key: priv key bits set: 137/256
debug2: bits set: 1022/2048
debug1: expecting SSH2_MSG_KEX_DH_GEX_INIT
debug2: bits set: 1022/2048
debug1: SSH2_MSG_KEX_DH_GEX_REPLY sent
debug2: kex_derive_keys
debug2: set_newkeys: mode 1
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug2: set_newkeys: mode 0
debug1: SSH2_MSG_NEWKEYS received
debug1: KEX done
debug1: userauth-request for user user1 service ssh-connection method
none
debug1: attempt 0 failures 0
debug2: input_userauth_request: setting up authctxt for user1
debug1: PAM: initializing for "user1"
debug3: PAM STARTS FROM HERE
debug3: Trying to reverse map address 127.0.0.1.
debug1: PAM: setting PAM_RHOST to "localhost"
debug1: PAM: setting PAM_TTY to "ssh"
debug2: input_userauth_request: try method none
debug3: DOOPIE!###!
Failed none for user1 from 127.0.0.1 port 32861 ssh2
```

Re: Confounded by PAM and OpenSSH on Solaris 10

```
debug1: userauth-request for user user1 service ssh-connection method
keyboard-interactive
debug1: attempt 1 failures 1
debug2: input_userauth_request: try method keyboard-interactive
debug1: keyboard-interactive devs
debug1: auth2_challenge: user=user1 devs=
debug1: kbdint_alloc: devices 'pam'
debug2: auth2_challenge_start: devices pam
debug2: kbdint_next_device: devices <empty>
debug1: auth2_challenge_start: trying authentication method 'pam'
debug3: PAM: sshpam_init_ctx entering
debug3: sshpam_thread called!!!!!!!
debug3: PAM: sshpam_thread_conv entering, 1 messages
debug3: ssh_msg_send: type 1
debug3: ssh_msg_recv entering
debug3: PAM: sshpam_query entering
debug3: ssh_msg_recv entering
debug3: DOOPIE!#!#!
Postponed keyboard-interactive for user1 from 127.0.0.1 port 32861 ssh2
debug2: PAM: sshpam_respond entering, 1 responses
debug3: ssh_msg_send: type 6
debug3: POOPIE!@!@!
debug1: do_pam_account: called
debug3: PAM: sshpam_thread_conv entering, 1 messages
debug3: ssh_msg_send: type 3
debug3: PAM: do_pam_account pam_acct_mgmt = 17 (User account has
expired)
debug3: ssh_msg_send: type 9
debug3: PAM: sshpam_query entering
debug3: ssh_msg_recv entering
debug3: ssh_msg_recv entering
debug3: PAM: PAM_AUTH_ERR
debug3: DOOPIE!#!#!
Postponed keyboard-interactive/pam for user1 from 127.0.0.1 port 32861
ssh2
debug2: PAM: sshpam_respond entering, 0 responses
debug2: auth2_challenge_start: devices <empty>
debug3: PAM: sshpam_free_ctx entering
debug3: PAM: sshpam_thread_cleanup entering
debug3: DOOPIE!#!#!
Failed keyboard-interactive/pam for user1 from 127.0.0.1 port 32861
ssh2
debug1: userauth-request for user user1 service ssh-connection method
keyboard-interactive
debug1: attempt 2 failures 2
debug2: input_userauth_request: try method keyboard-interactive
debug1: keyboard-interactive devs
debug1: auth2_challenge: user=user1 devs=
debug1: kbdint_alloc: devices 'pam'
debug2: auth2_challenge_start: devices pam
debug2: kbdint_next_device: devices <empty>
```

Re: Confounded by PAM and OpenSSH on Solaris 10

```
debug1: auth2_challenge_start: trying authentication method 'pam'
debug3: PAM: sshpam_init_ctx entering
debug3: sshpam_thread called!!!!!!!
debug3: PAM: sshpam_thread_conv entering, 1 messages
debug3: ssh_msg_send: type 1
debug3: ssh_msg_recv entering
debug3: PAM: sshpam_query entering
debug3: ssh_msg_recv entering
debug3: DOOPIE!#!#!
Postponed keyboard-interactive for user1 from 127.0.0.1 port 32861 ssh2
debug2: PAM: sshpam_respond entering, 1 responses
debug3: ssh_msg_send: type 6
debug3: PAM: sshpam_query entering
debug3: ssh_msg_recv entering
debug3: POOPIE!@!@!
debug1: do_pam_account: called
debug3: PAM: sshpam_thread_conv entering, 1 messages
debug3: ssh_msg_send: type 3
debug3: ssh_msg_recv entering
debug3: PAM: do_pam_account pam_acct_mgmt = 17 (User account has
expired)
debug3: ssh_msg_send: type 9
debug3: PAM: PAM_AUTH_ERR
debug3: DOOPIE!#!#!
Postponed keyboard-interactive/pam for user1 from 127.0.0.1 port 32861
ssh2
debug2: PAM: sshpam_respond entering, 0 responses
debug2: auth2_challenge_start: devices <empty>
debug3: PAM: sshpam_free_ctx entering
debug3: PAM: sshpam_thread_cleanup entering
debug3: DOOPIE!#!#!
Failed keyboard-interactive/pam for user1 from 127.0.0.1 port 32861
ssh2
debug1: userauth-request for user user1 service ssh-connection method
keyboard-interactive
debug1: attempt 3 failures 3
debug2: input_userauth_request: try method keyboard-interactive
debug1: keyboard-interactive devs
debug1: auth2_challenge: user=user1 devs=
debug1: kbdint_alloc: devices 'pam'
debug2: auth2_challenge_start: devices pam
debug2: kbdint_next_device: devices <empty>
debug1: auth2_challenge_start: trying authentication method 'pam'
debug3: PAM: sshpam_init_ctx entering
debug3: sshpam_thread called!!!!!!!
debug3: PAM: sshpam_query entering
debug3: ssh_msg_recv entering
debug3: PAM: sshpam_thread_conv entering, 1 messages
debug3: ssh_msg_send: type 1
debug3: ssh_msg_recv entering
debug3: DOOPIE!#!#!
```

Re: Confounded by PAM and OpenSSH on Solaris 10

```
Postponed keyboard-interactive for user1 from 127.0.0.1 port 32861 ssh2
debug2: PAM: sshpam_respond entering, 1 responses
debug3: ssh_msg_send: type 6
debug3: PAM: sshpam_query entering
debug3: ssh_msg_recv entering
debug3: POOPIE!@!@!
debug1: do_pam_account: called
debug3: PAM: sshpam_thread_conv entering, 1 messages
debug3: ssh_msg_send: type 3
debug3: PAM: do_pam_account pam_acct_mgmt = 17 (User account has
expired)
debug3: ssh_msg_send: type 9
debug3: ssh_msg_recv entering
debug3: PAM: PAM_AUTH_ERR
debug3: DOOPIE!#!#!
Postponed keyboard-interactive/pam for user1 from 127.0.0.1 port 32861
ssh2
debug2: PAM: sshpam_respond entering, 0 responses
debug2: auth2_challenge_start: devices <empty>
debug3: PAM: sshpam_free_ctx entering
debug3: PAM: sshpam_thread_cleanup entering
debug3: DOOPIE!#!#!
Failed keyboard-interactive/pam for user1 from 127.0.0.1 port 32861
ssh2
Connection closed by 127.0.0.1
debug1: do_cleanup
debug1: PAM: cleanup
debug3: PAM: sshpam_thread_cleanup entering
[Mon May 01|14:18:11][root@unknown:/]
$
### END sshd debug ###
```

If you look at the sshd debug you will see that my pam module returns "debug3: PAM: do_pam_account pam_acct_mgmt = 17 (User account has expired)" however the user is prompted again for a password. I looked at the code and found that do_pam_account() is called from sshpam_thread(void *ctxtp). There seems to be no code that kicks the user out after a bad attempt it just goes through the attempts cycle. I assume sshd checks the thread's return code this is how it knows whether or not the authentication was successful so it should be able to kick the user out.

```
### START code snippet ###
if (compat20) {
if (!do_pam_account())
goto auth_fail;
if (sshpam_authctx->force_pwchange) {
sshpam_err = pam_chauthtok(sshpam_handle,
PAM_CHANGE_EXPIRED_AUTHTOK);
if (sshpam_err != PAM_SUCCESS)
goto auth_fail;
```

Re: Confounded by PAM and OpenSSH on Solaris 10

```
sshpam_password_change_required(0);
}
}
auth_fail:
buffer_put_cstring(&buffer,
pam_strerror(sshpam_handle, sshpam_err));
/* XXX – can't do much about an error here */
ssh_msg_send(ctxt->pam_csock, PAM_AUTH_ERR, &buffer);
buffer_free(&buffer);
pthread_exit(NULL);

return (NULL); /* Avoid warning for non-threads case */
}
### END code snippet ###
```

If you look at auth2.c in userauth_finish() the code checks for errors...

```
### START code snippet ###
#ifdef USE_PAM
debug3( "DOOPIE!#!#!" );
if (options.use_pam && authenticated) {
if (!PRIVSEP(do_pam_account())) {
/* if PAM returned a message, send it to the user */
if (buffer_len(&loginmsg) > 0) {
buffer_append(&loginmsg, "\0", 1);
userauth_send_banner(buffer_ptr(&loginmsg));
packet_write_wait();
}
fatal("Access denied for user %s by PAM account "
"configuration", authctxt->user);
}
}
#endif
### END code snippet ###
```

Here there is a fatal statement saying that access is denied, which I assume kicks you out.

```
SSHD CONFIGURATION #3
Protocol 2
PasswordAuthentication no
ChallengeResponseAuthentication yes
UsePAM yes
```

```
user1 now prompts 4 times three times for keyboard-interactive and once
for password.
#####
```

Re: Confounded by PAM and OpenSSH on Solaris 10

[Fri Apr 28|19:24:50][root@unknown:/]

\$ ssh -l user1 localhost

Password:

User account has expired!

Password:

User account has expired!

Password:

User account has expired!

user1@localhost's password:

User account has expired!

Are you sure about this one? If PasswordAuthentication is set to no, it won't even be offered to the client.

I wonder if "UsePrivilegeSeparation yes" had anything to do with it?

Elroy

.